Auto-Cascading Security Updates Through Docker Images

Andrey Falko

Salesforce Infrastructure
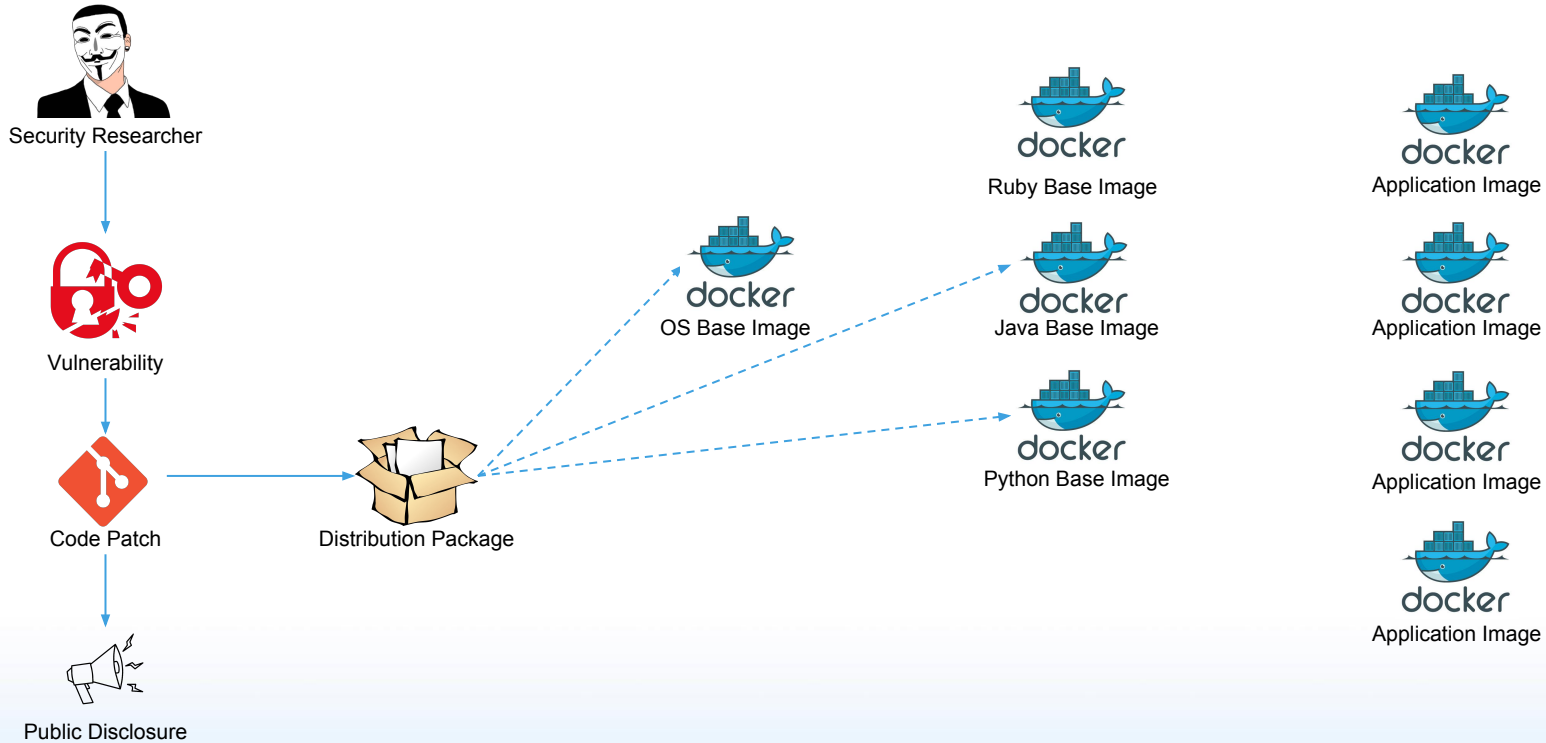
Forward-Looking Statements

Statement under the Private Securities Litigation Reform Act of 1995:

This presentation may contain forward-looking statements that involve risks, uncertainties, and assumptions. If any such uncertainties materialize or if any of the assumptions proves incorrect, the results of salesforce.com, inc. could differ materially from the results expressed or implied by the forward-looking statements we make. All statements other than statements of historical fact could be deemed forward-looking, including any projections of product or service availability, subscriber growth, earnings, revenues, or other financial items and any statements regarding strategies or plans of management for future operations, statements of belief, any statements concerning new, planned, or upgraded services or technology developments and customer contracts or use of our services.
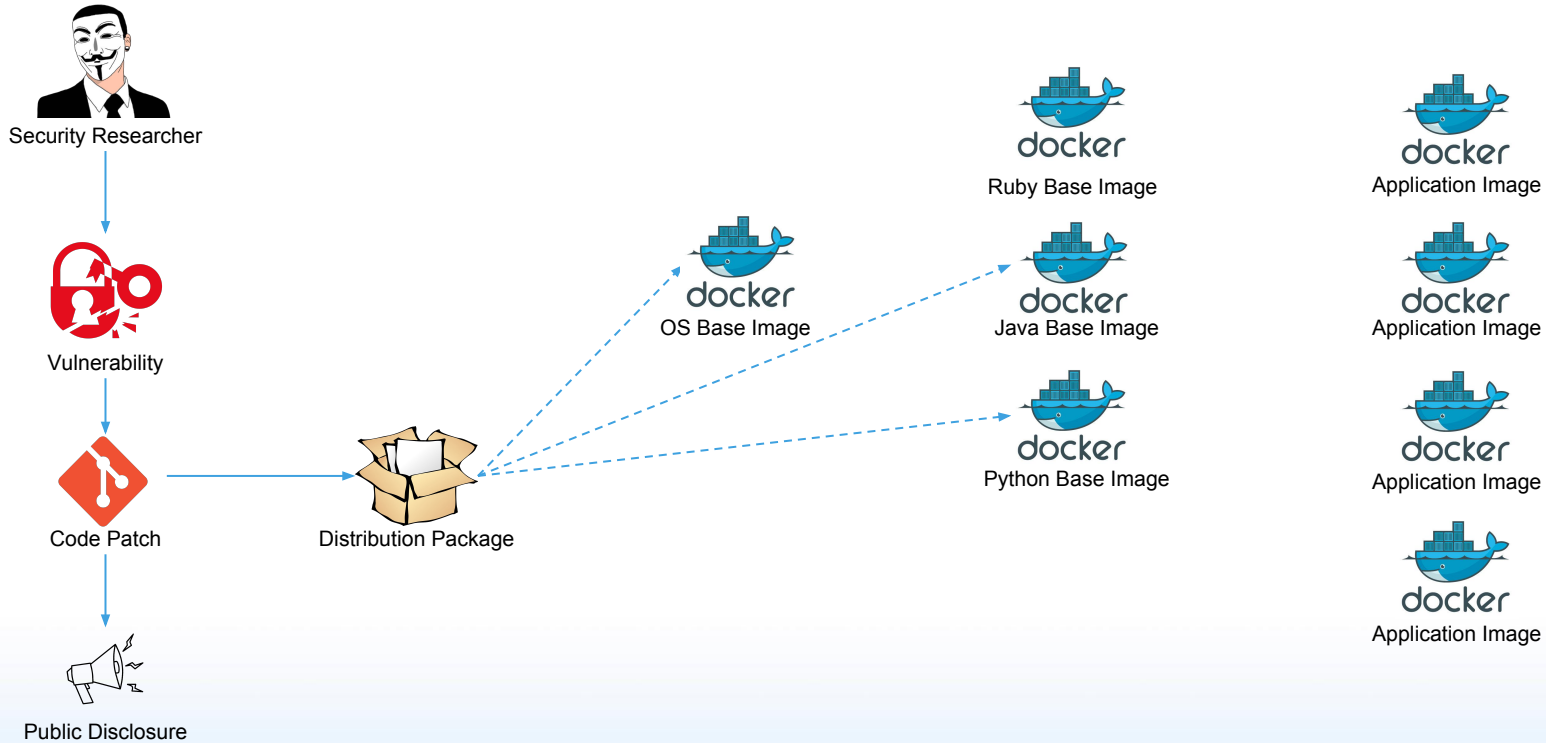
The risks and uncertainties referred to above include – but are not limited to – risks associated with developing and delivering new functionality for our service, new products and services, our new business model, our past operating losses, possible fluctuations in our operating results and rate of growth, interruptions or delays in our Web hosting, breach of our security measures, the outcome of any litigation, risks associated with completed and any possible mergers and acquisitions, the immature market in which we operate, our relatively limited operating history, our ability to expand, retain, and motivate our employees and manage our growth, new releases of our service and successful customer deployment, our limited history reselling non-salesforce.com products, and utilization and selling to larger enterprise customers. Further information on potential factors that could affect the financial results of salesforce.com, inc. is included in our annual report on Form 10-K for the most recent fiscal year and in our quarterly report on Form 10-Q for the most recent fiscal quarter. These documents and others containing important disclosures are available on the SEC Filings section of the Investor Information section of our Web site.

Any unreleased services or features referenced in this or other presentations, press releases or public statements are not currently available and may not be delivered on time or at all. Customers who purchase our services should make the purchase decisions based upon features that are currently available. Salesforce.com, inc. assumes no obligation and does not intend to update these forward-looking statements.

The problem

Security Researcher

Vulnerability

Code Patch

Public Disclosure

Distribution Package

OS Base Image

Ruby Base Image

Java Base Image

Python Base Image

Application Image
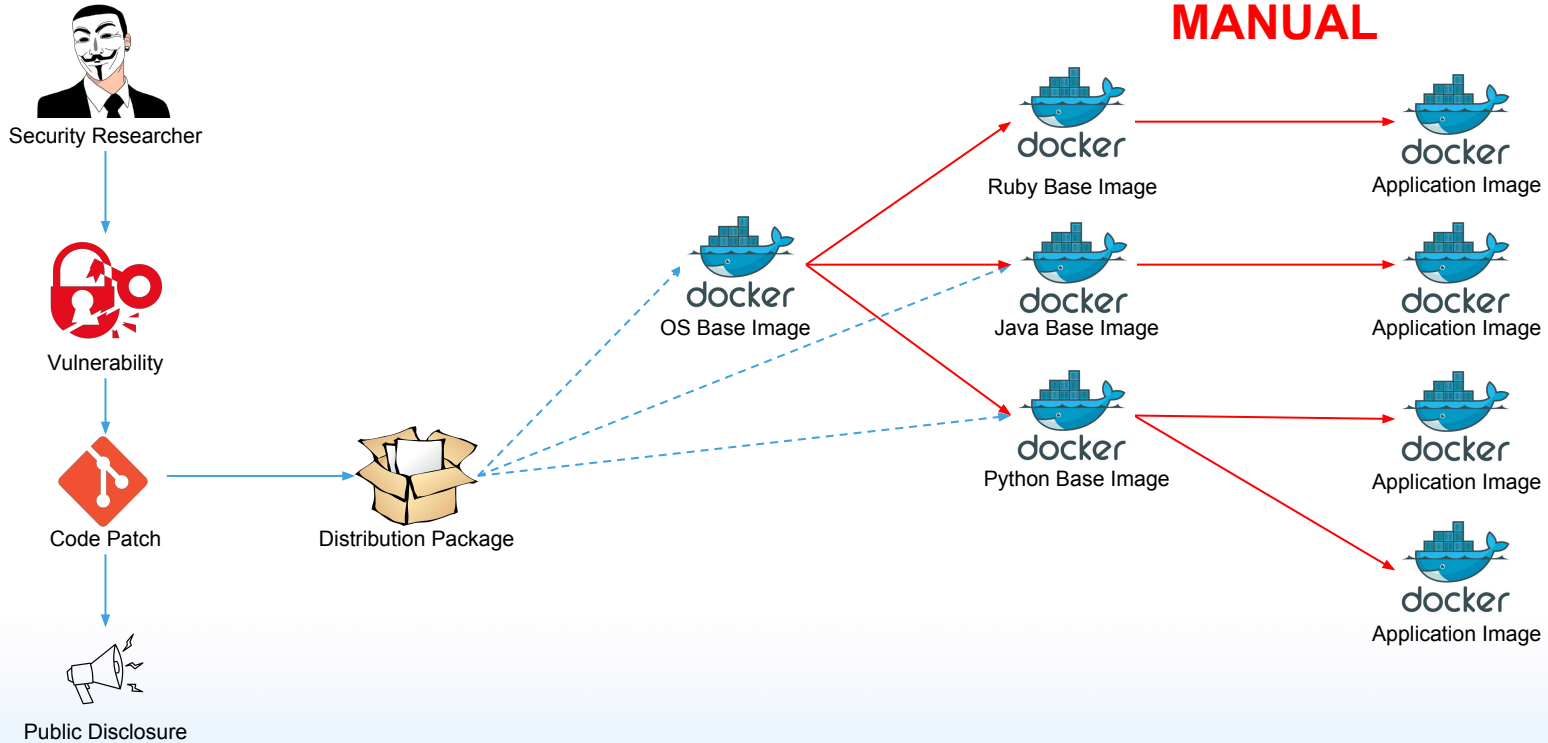
Application Image

Application Image

Application Image
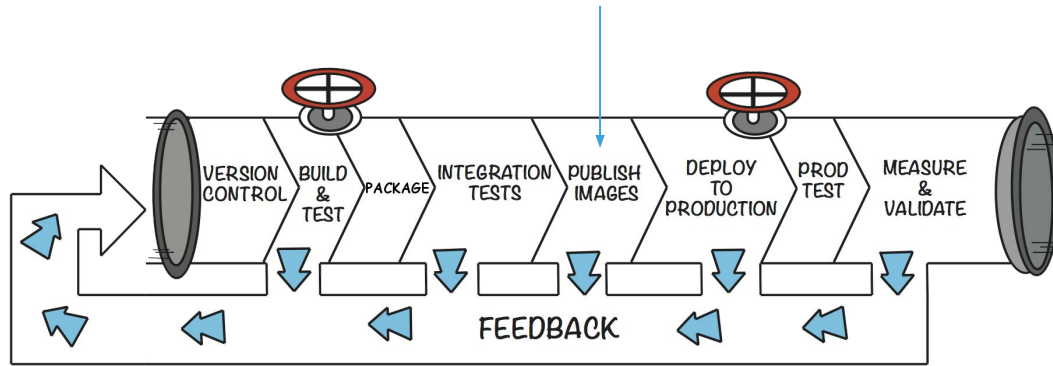
The problem

The problem

Our Solution

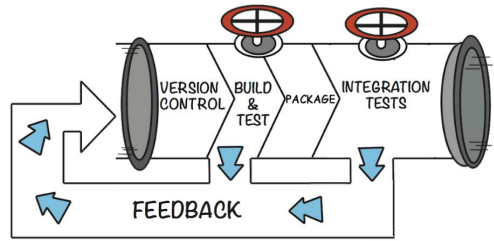How do you automatically keep all of these images up-to-date?

Create Pull Request to every child image

Our Solution

We run tests for our pull requests

Pull request pipeline

Developer review and merge
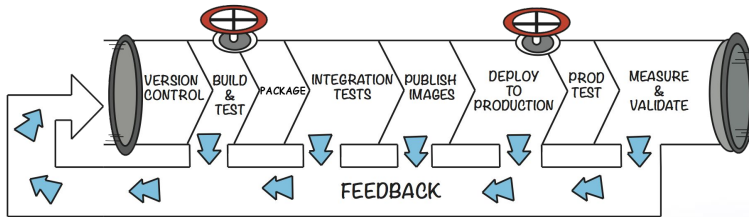
Path to production

Our Solution: Dockerfile Image Update

Command line tool invoked as Docker container

```
# dockerfile-image-update parent <PARENT-IMG> <VERSION-TAG> <IMG_TAG_STORE-GIT-REPO>
```

- PARENT-IMG - Base image whose children we want to update
- VERSION-TAG - Docker tag that we intend children to be updated to
- IMG_TAG_STORE-GIT-REPO - Git repository where you want to persist intended outcome

Our Solution: Dockerfile Image Update

Command line tool invoked as Docker container

```
# dockerfile-image-update parent <PARENT-IMG> <VERSION-TAG> <IMG_TAG_STORE-GIT-REPO>
```

- PARENT-IMG - Base image whose children we want to update
- VERSION-TAG - Docker tag that we intend children to be updated to
- IMG_TAG_STORE-GIT-REPO - Git repository where you want to persist intended outcome

Our Solution: Dockerfile Image Update

Command line tool invoked as Docker container

Example:

```
                                                                Command Line
# dockerfile-image-update parent centos_jdk 8 version-persistence-repo
```

We open sourced it: **https://github.com/salesforce/dockerfile-image-update**

Our Solution

Why do we need to track image versions?

```
# dockerfile-image-update all <IMG_TAG_STORE-GIT-REPO>
```

- Scans all images in IMG_TAG_STORE and updates child images
- Run nightly for all images
    - Ensures no one bypassed CI system
    - Developer race conditions
    - Github can't fork a fork

Our Solution

Why do we need to track image versions?

```
                                                              Command Line
# dockerfile-image-update all <IMG_TAG_STORE-GIT-REPO>
```

- Scans all images in IMG_TAG_STORE and updates child images
- Run nightly for all images
    - Ensures no one bypassed CI system
    - Developer race conditions
    - Github can't fork a fork

The Result

Software that writes code

Automatic Dockerfile Image Updater #2

Edit

Open dockerfile-imag... wants to merge 8 commits into `afalko:master` from `dockerfile-image-update-service:master`

Conversation 0   Commits 8   Files changed 1

Changes from **all commits** ▾   Jump to... ▾   **+1 −1** ▪▪▫▫▫

Unified   **Split**   **Review changes** ▾

2 ▪▪▫▫▫ Dockerfile   View ✏ ⌄

```
        @@ -1,4 +1,4 @@
1       -FROM afalko/alpine-java:10
     1  +FROM afalko/alpine-java:18
2    2
3    3   LABEL version="0.1"
4    4
```

The Result

I had an uninterrupted vacation in Florida

The Result

In all seriousness...

- Hundreds of docker images are patched using this tool
- Hundreds of developers migrated services to major OS and language versions safely

Future Improvements

What we can do better

- Users and Contributors Welcome!
  - https://github.com/salesforce/dockerfile-image-update
- Feature wishlist:
  - Auto-merge option
  - Maven spotify docker plugin support
  - Update versions in docker-compose and kubernetes pod.yaml
  - Expand the tool to other packaging formats beyond just Docker

Future Improvements

What we can do better

- Users and Contributors Welcome!
  - https://github.com/salesforce/dockerfile-image-update
- Feature wishlist:
  - Auto-merge option
  - Maven spotify docker plugin support
  - Update versions in docker-compose and kubernetes pod.yaml
  - Expand the tool to other packaging formats beyond just Docker

Future Improvements

What we can do better

- Users and Contributors Welcome!
  - https://github.com/salesforce/dockerfile-image-update
- Feature wishlist:
  - Auto-merge option
  - Maven spotify docker plugin support
  - Update versions in docker-compose and kubernetes pod.yaml
  - Expand the tool to other packaging formats beyond just Docker

Future Improvements

What we can do better

- Users and Contributors Welcome!
  - https://github.com/salesforce/dockerfile-image-update
- Feature wishlist:
  - Auto-merge option
  - Maven spotify docker plugin support
  - Update versions in docker-compose and kubernetes pod.yaml
  - Expand the tool to other packaging formats beyond just Docker

Thank you!

Wouldn't be possible without these Engineers

- Former Salesforce intern wrote initial version
  - Min Ho Park
- Helped with design, fixes, and production support
  - Justin Harringa
  - Nelson Wolf
  - Jinesh Doshi

THANK YOU

https://github.com/salesforce/dockerfile-image-update